Projektni zadatak 12.

Potrebno je implementirati servis koji ima ulogu *Domen Kontroler* (DC) komponente i predstavlja treću stranu od poverenja prilikom uspostavljanja bezbedne komunikacije između klijenta i servisa. DC se sastoji iz dve komponente:

- *Authentication Service (AS):*
  - Predstavlja skladište korisničkih naloga, i klijentskih i servisnih (šifre se ne smeju skladištiti u čitljivom formatu
- *Ticket Granting Service (TGS):*
  - Sadrži DNS tabelu (odnosno, par IPAdresa:hostName), kao i evidenciju o startovanim servisima u domenu (IP adresa/hostname i identitet servisa)

Prilikom uspostavljanja komunikacije, klijent se usmerava ka AS komponenti za autentifikaciju. U slučaju uspešne autentifikacije, zahtev se šalje ka TGS komponenti koji proverava da li postoji zahtevani servis u domenu. Ukoliko servis postoji, TGS generiše tajni ključ koji klijent i servis koriste dalje u procesu ostvarivanja bezbedne komunikacije komunikaciji. Neophodno je obezbediti poverljivost prilikom razmena tajnog ključa između TGS i klijenta, odnosno TGS i servisa. Klijent i servis potvrđuju svoj identitet po principu challenge-response protokola, kada se razmenjuje i njihov ključ sesije.

DC loguje u specifičnom Windows event logu bezbednosne događaje koji se odnose na uspostavljanje komunikacije:

- Uspešna ili neuspešna autentifikacija klijenta na AS komponenti
- Uspešna ili neuspešna validacija servisa na TGS komponenti

Servis implementira interfejs *IDataManagement* koji nudi dve metode za rad sa bazom podataka u kojoj se skladište poverljivi podaci:

- Read() – čitanje podataka iz baze podataka
- Write() – upis u bazu podataka.

U okviru ovih metoda podaci se prilikom razmene kriptuju primenom 3DES algoritma u CBC modu (ugrađeni .NET mehanizam) koristeći razmenjeni ključ sesije kao tajni ključ.